Administrative

Project Title:

A toolbox for verification of embedded control system designs

Approved for Public Release, Distribution Unlimited

Subcontractors and Collaborators

- **Carnegie Mellon University**

  Peter Feiler (SEI)

- **Emmeskay, Inc.**

  Shiva N. Sivashankar

  Swami Gopalswamy

- **The MathWorks, Inc.**

  Mehran Mestchian

  William Aldrich

Technical Problems

- many models are create of *the same system* to evaluate embedded control designs
  - models are created and managed manually
- simulation is used extensively
  - exploration of design is ad hoc
  - results are managed manually
- model checking shows some promise
  - custom models need to be constructed manually
  - verification problem has to be very focused to be tractable

Project goal: To create a MATLAB Toolbox that supports the integrated use of new simulation-based and formal methods for analysis and verification of embedded control system designs

Project Team - Roles

- CMU – Technology development
  - simulation & model checking methods (Krogh)
  - model relations manager (Feiler)
  - prototypes & case studies
- Emmeskay – Software development
  - toolbox design and implementation
  - testing and evaluation
- MathWorks – Environment expertise
  - design guidelines/advice
  - special purpose APIS

Contribution to Goals of MoBIES

BAA #02-11 Topic 1. Analysis and Design Tools

... tools for verification and validation

... tools spanning other constraints and requirements of embedded applications are encouraged

... open data formats

... expertise in physical phenomena of interest to embedded software developers

... interface to other MoBIES components through common interface such as those based on Matlab/Simulink/Stateflow

... open, extensible, well-documented formats, compliant with the standards MoBIES is developing

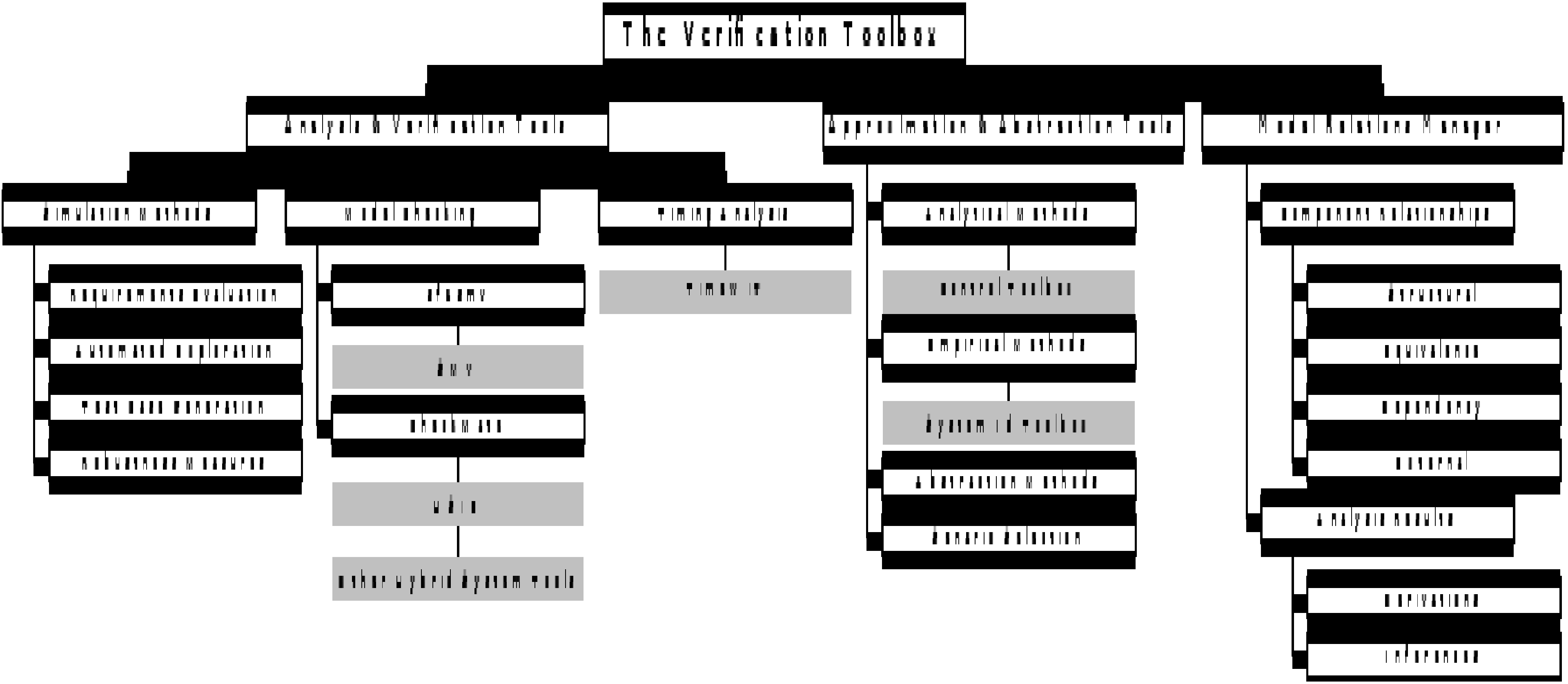
The Verification Toolbox

- Simulation-Based Analysis
  - automatic generation of simulation experiments
  - global search methods for exploration of the operating space and test case generation
  - perturbation-based generation of robustness measures
- Model Checking
  - projections and compositional reasoning for decomposition
  - abstraction refinement based on counterexamples analysis
  - focused model checking based on integrated simulation analysis and user guidance

The Verification Toolbox – cont'd.

- Model Approximation and Abstraction
  - generate model abstractions for formal analysis directly from existing design models
  - library of analytical, empirical, and scenario-based methods
- Model Relations Manager
  - representations for maintaining and inferring knowledge from verification studies, incorporating user-supplied domain knowledge
  - maintain model consistency information as are modified
  - generate timing models for target platform

Elements of the Verification Toolbox



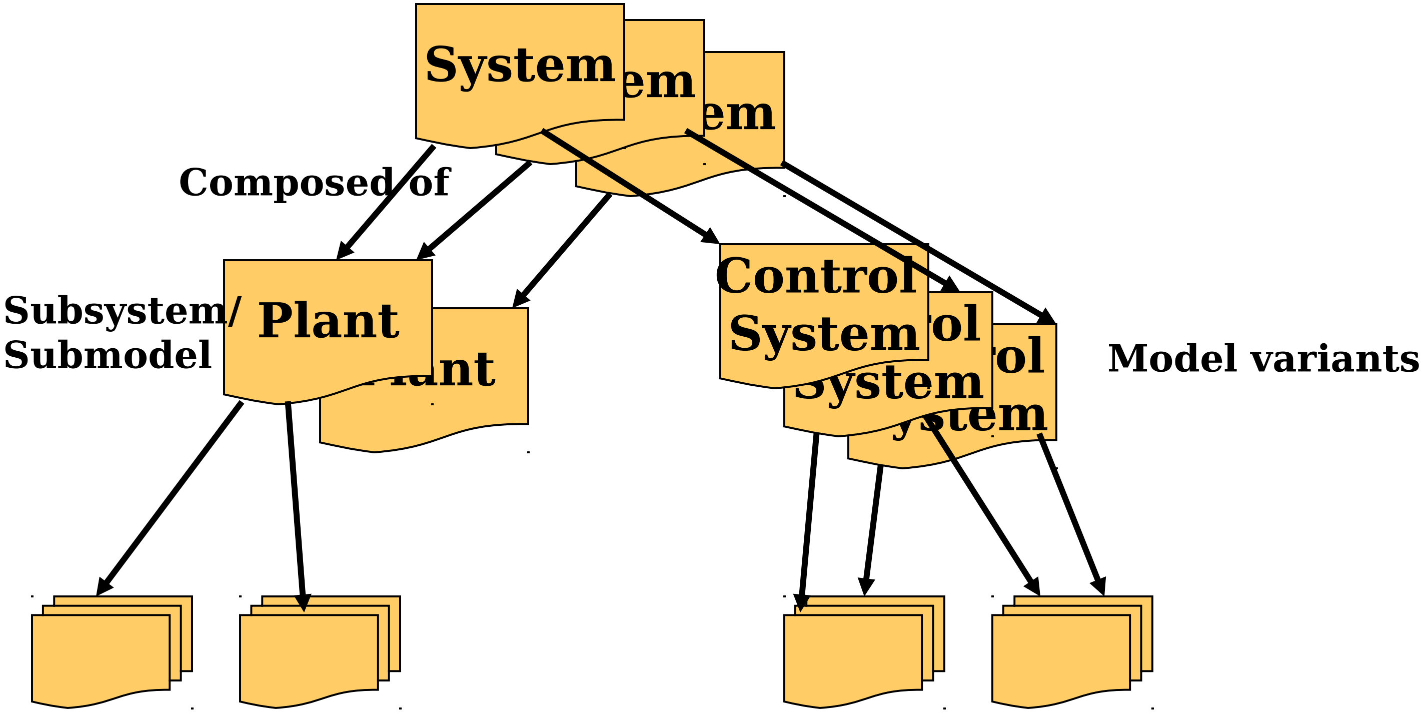
Electrical & Computer ENGINEERING

MoBIES

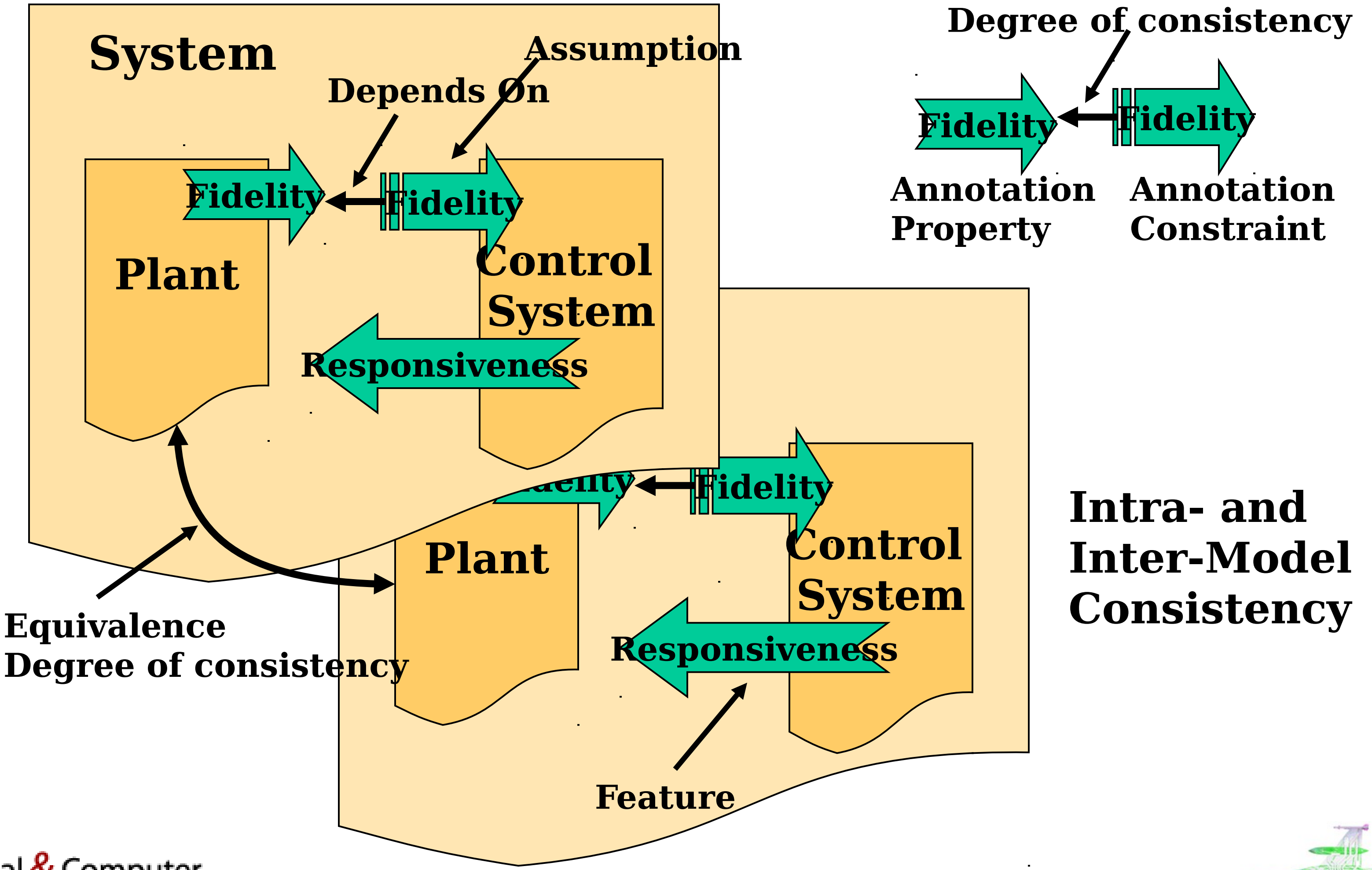
Model Relations Manager

- Families of System Models
  - System Architecture and Compositional Relations
  - Model Variants
- Features and Consistency
  - Assumptions and Dependency Relations
  - Annotations and Constraints
  - Equivalence Relations on Model Variants
  - Consistency and degrees of importance
- Managing Analysis Results
  - Simulation & Analysis Results and Derivation Relations
  - Observations and Inference Relations

Families of System Models



Features and Consistency



System

Assumption

Depends On

Fidelity

Fidelity

Plant

Control System

Responsiveness

idelity

Fidelity

Plant

Control System

Responsiveness

Equivalence
Degree of consistency

Feature

Degree of consistency

Fidelity

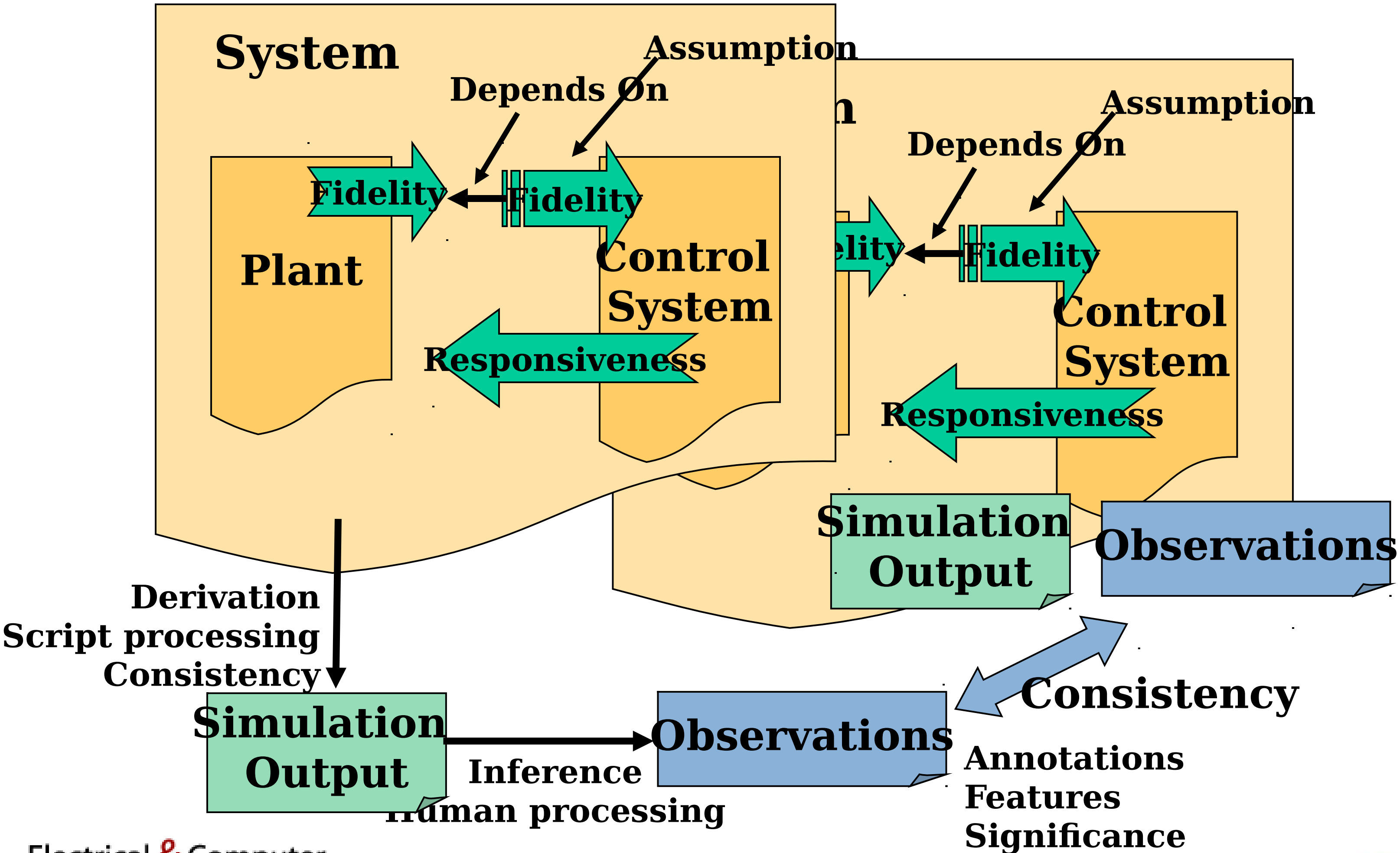
Fidelity

Annotation
Property

Annotation
Constraint

Intra- and
Inter-Model
Consistency

Managing Analysis Results



System

Assumption

Depends On

Fidelity

Fidelity

Plant

Control System

Responsiveness

n

Assumption

Depends On

elity

Fidelity

Control System

Responsiveness

Simulation Output

Observations

Derivation
Script processing
Consistency

Simulation Output

Inference
Human processing

Observations

Consistency

Annotations
Features
Significance

Relationships to other Work

- Version & configuration management
  - AND/OR graph based composition
- Software system build
  - Composition structure & derivation
- Architecture Description Languages (ADL)
  - Structure, interaction dependency, analysis & generation
  - Real-time: Images TimeWeaver, Honeywell MetaH
- ADL and domain semantics (EDCS INSERT)
  - Hidden side effects and impact analysis
- Mobies AMC (Model Compiler)
  - domain semantic constraint-based composition

OEP Participation

Automotive OEP

- leverage experience with verification of ETC
- new power train applications

Project Plans – next 6 months

- Implementation
  - functional design & architecture
- Analysis techniques
  - simulation-based exploration
  - focused model checking
- Model Management
  - model relations representation

Project Schedule and Milestones

	Year 1				Year 2			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Task 1. Toolbox Implementation								
1.1 Functional Design	▨	▨						
1.2 Implementation Architecture		▨	▨					
1.3 Implement Mod. Relations Manager			▨	▨	▨	▨		
1.4 Implement Anal. & Abstract. Tools					▨	▨	▨	▨
1.5 Extensibility Features							▨	▨
1.6 User Documentation							▨	▨
Task 2. Anal. & Abstract. Methods								
2.1 Simulation-Based Verification	▨	▨	▨	▨				
2.2 Focused Model Checking	▨	▨	▨	▨				
2.3 Counterexample Discovery/Exploit.				▨	▨	▨		
2.4 Timing Specifications & Analysis						▨	▨	
2.5 Model Approx. & Abstraction				▨	▨			
2.6 Model-Based Test Case Generation				▨	▨			

Project Schedule and Milestones- cont'd

Task 3. Model Represent. and Relations									
3.1 Model Relations Representation		▨	▨						
3.2 Representing Specs. & Coverage						▨	▨	▨	
3.3 Relations from Approx. & Abstract.				▨	▨	▨	▨		
3.4 Relations from Analysis					▨	▨	▨		
Task 4. Testing and Evaluation									
4.1 Code Testing & Debugging				▨	▨			▨	▨
4.2 OEP Applications- Models				▨	▨	▨	▨		
4.3 OEP Applications- Analysis							▨	▨	▨
4.4 Demonstrations						▨	▨		▨

Technology Transition/Transfer

- Related projects
  - Ford Motor Co.
  - Lockheed-Martin
  - Honeywell
- Software development/support – Emmeskay
- Goal: Full-fledged MATLAB toolbox